



**RISK MANAGEMENT INFORMATION**  
**COMPUTER LOSS CONTROL**

As more cities find ways to increase efficiency and communications through technology, the need for better computer security grows. Even if a city has just one computer, if the city stores valuable data on the system or connects to the Internet it might be exposed to computer threats. Not doing anything could open the city to disastrous consequences.

This memo lists some of the possible risks associated with computer use and then lists recommendations to reduce these risks. The recommendations discussed in this memo are not a guarantee that your computer system is completely safe from harm. The best way to make sure your city is protected is to keep up with new developments in this area. One good way to sort through all the technical information available is by signing up to be part of the League's new Computer Security Listserv. (Log on to <http://www.lmc.org/forms/listserv.cfm>)

**Possible risks associated with poor computer security are:**

**Virus contamination of computer files** that may cause havoc in two ways:

- Destroying the city's data including financial information, citizen information and employee records. This would cost the city a lot of money in reconstructing data and software.
- Sending itself to everyone in the users' address books, and destroying others' data and software. The affected party may sue the city for negligently allowing the virus to be transmitted.

**Hacker attack of the city's system**, including scenarios such as:

- Obtaining private data. The subject of the data sues the city for allowing the data to become public.
- Destroying or modifying city data.
- Hijacking the city's system to use it for a "denial of service" attack on a third party.
- The affected party in turn sues the city for carelessness in allowing computers to be so easily commandeered by the hacker.

**Loss of data and software** stemming from an accident such as an all-consuming fire at City Hall. Data and software cannot be recovered.

This material is provided as general information and is not a substitute for legal advice.  
Consult your attorney for advice concerning specific situations.

**Misuse of city's computers**, such as:

- City employee using the city's computer to send harassing e-mails.
- City employee's expectation of privacy in e-mail communications. An employee may sue the city for looking at the e-mails the employee sent or received on the city's system, claiming that he expected those communications to be treated as private.

**Web site information** that pinpoints the location, size and design of the city's water system facilities or emergency response practices. This information is used by a terrorist organization to plan an attack.

**Discovery demand for information may include all the city's relevant e-mails**, including those that are or may be contained on the back-up tapes from the past several years. The city may spend significant time and money looking for the relevant e-mails on the back-up tapes, and separating them from the private and non-public data that's on those same tapes.

**Disability due to bad ergonomics**, for instance, a city employee who is permanently disabled by repetitive stress syndrome from using a badly-designed workstation. This may result in a very expensive work comp claim for the city.

**Following are concrete recommendations to reduce these risks.**

**Ensure all computers used for city business (including ones at home if used to do city work) have anti-virus software installed on them. In addition, any computer that can connect to the Internet needs to be secured with firewall protection.** Although these measures are not going to protect the city 100 percent from all viruses or hacker attacks, they will make it harder to get into the city's system and may encourage a hacker to look elsewhere for an easier target. Cities are encouraged to consider consulting or contracting with a technology professional to assure that the systems are adequately installed and maintained.

- **Anti-virus software** offers protection against most known viruses by attempting to identify and neutralize them. Cities should purchase and regularly update anti-virus software so that it is effective against new viruses that are created literally daily to attack computers. It is critical to set this software to automatically screen incoming and outgoing e-mails and attachments.

Anti-Virus software is available from a variety of vendors. Select anti-virus software from a reputable vendor that provides support in the event of a virus outbreak. Some of the most common software vendors include Symantec, McAfee and Computer Associates. Another option in addition to installing virus software is to use a company such as MessageLabs to screen all incoming and outgoing e-mails, or install an internal e-mail scanning tool such as GFI's Mail Essentials. .

- **Installing a firewall** makes it difficult for a hacker to break into the city's computer system by effectively creating a barrier. A firewall masks all the information and activity on your side of the modem from the Internet—many anti-virus software companies are encouraging you to purchase firewalls, and some are including it in upgrades to existing anti-virus software.

If the city connects to the Internet in any way (dial-up modem, dedicated line, etc.) it is recommended to have firewall software in place. Install a firewall and keep current. Firewalls can be set up as hardware or software.

Ensure that the firewall is properly configured. Misconfigured firewalls can be just as risky as not having a firewall at all.

If you only have a single computer connecting to the Internet, utilize the built in firewall, or purchase a software firewall from a reputable vendor.

- **Patches, services packs and upgrades** need to be applied regularly to all operating systems, computer connectivity equipment such as routers, and desktop applications. If possible these updates should be automated, and end users should not be given a choice of running the updates. These products are designed to fix security issues, improve programs and fill in the gaps. Applying patches for any Microsoft operating system or application can be accomplished by utilizing the Microsoft update product, found at [www.windowsupdate.com](http://www.windowsupdate.com). Updating and patching virus software is also a fairly automated process and should be able to be accomplished by a staff member.

**Regularly backup the data on the city's computers and test to insure backups are not corrupted.** The city should backup all data to protect itself from natural disaster, failed hardware, viruses, or hacker attacks. Backup media should be stored in a secure climate controlled off site location. Storing backup media in the back of a public works shed would probably not fit the definition of a secure climate controlled off site location.

The city should establish a regular backup schedule addressing frequency of backups and retention of backup media. Backups should be done on a daily basis. A complete monthly backup should be maintained on a 12-month rotating schedule. Ultimately, the type of schedule really depends on the size of the city and the kind of operations housed in the system.

Backup media should be replaced on an annual basis. Most backup media will deteriorate after a year of use.

**Address how e-mails and backup tapes containing e-mails are handled in the city's records retention schedule.** Cities should back up e-mail separately, so that e-mails aren't retained indefinitely along with other city data that has a longer retention need. A separate e-mail backup also ensures any archived electronic city records do not need to be searched as part of an e-mail e-discovery ordered by the court.

**Adopt a computer use policy.** Make sure city employees are aware of the policy, and consistently enforce it. A policy sample and considerations are available from The League of Minnesota Cities.

**Think about the kind of information posted in the city's web site.** Some recommendations are:

- Make sure there's no private data.
- Make sure the information is accurate.

- Even if data is legally public (e.g., the location, size, and design of your water system) it may not be a good idea to post it on the web site. Only post information that is legitimately useful to citizens and constituents.

Greg Van Wormer 11/06/07